

Notice of References Cited	Application/Control No. 09/786,756	Applicant(s)/Patent Under Reexamination KNUDSEN, ERIK	
	Examiner Michael J Simitoski	Art Unit 2134	Page 1 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,141,420 A	10-2000	Vanstone et al.	380/30
	B	US-6,490,352 B1	12-2002	Schroeppel, Richard	380/30
	C	US-2002/0041681	04-2002	Hoffstein et al.	380/28
	D	US-2002/0055962 A1	05-2002	Schroeppel, Richard	708/650
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Avanzi, Roberto M. et al. "SCALAR MULTIPLICATION ON KOBLITZ CURVES USING THE FROBENIUS ENDOMORPHISM AND ITS COMBINATION WITH POINT HALVING: EXTENSIONS AND MATHEMATICAL ANALYSIS", 2003.
	V	Fong, Kenny et al. "Field Inversion and Point Halving Revisited", August 2004, IEEE Transactions on Computers Vol. 58, No. 8.
	W	Gunther, Christian et al. "Speeding up the Arithmetic on Koblitz Curves of Genus Two", SAC 2000, August 2000.
	X	Jacobson, Michael, Jr. et al. "Hyperelliptic Curves and Cryptography", 2004.

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 09/786,756	Applicant(s)/Patent Under Reexamination KNUDSEN, ERIK	
	Examiner Michael J Simitoski	Art Unit 2134	Page 2 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Koblitz, Neal. "An Elliptic Curve Implementation of the Finite Field Digital Signature Algorithm", CRYPTO '98, 1998.
	V	Koblitz, Neal. "CM-Curves with Good Cryptographic Properties", CRYPTO '91, 1991.
	W	Meier, Willi et al. "Efficient Multiplication on Certain Nonsupersingular Elliptic Curves", CRYPTO '92, 1992.
	X	Schroeppel, Richard et al. "Fast Key Exchange with Elliptic Curve Systems", March 1995.

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 09/786,756	Applicant(s)/Patent Under Reexamination KNUDSEN, ERIK	
	Examiner Michael J Simitoski	Art Unit 2134	Page 3 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Solinas, Jerome A. "An Improved Algorithm for Arithmetic on a Family of Elliptic Curves", CRYPTO '97, 1997.
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.